Enterprise Risk Management – Aligning Risk with Strategy and Performance
COSO ERM Framework Update
April 4, 2017

Agenda

1. Setting the Stage for Enterprise Risk Management
2. Project Overview
3. Key Changes to the Framework
4. Public Exposure process
5. Next Steps
Setting the Stage for Enterprise Risk Management

The Strategic Value of Enterprise Risk Management

- Increases the range of opportunities
- Identifies and manages entity-wide risks
- Reduces surprises and losses
- Reduces performance variability
- Improves resource deployment
- Anticipates, identifies, adapts, and responds to change
A Key Introduction…

- Our understanding of the nature of risk, the art and science of choice lies at the core of our modern market economy.
- Every choice we make in the pursuit of objectives has its risks. From day-to-day operational decisions to the fundamental trade-offs in the boardroom, dealing with uncertainly in these choices is a part of our organizational lives.

Project Overview
Who is COSO?

- Refers to the Committee of Sponsoring Organizations of the Treadway Commission
- Established in 1985 as a joint initiative of five private sector organizations

States its mission as providing “thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations”.

Project to Update Enterprise Risk Management – Integrated Framework

- Announced in October 2014
- Update the 2004 Enterprise Risk Management–Integrated Framework
- Goal of:
  - Enhancing the framework’s content and relevance in an increasingly complex business environment
  - Enabling organizations worldwide to attain better value from their enterprise risk management practices
Why Update the ERM Framework Now

- Since 2004, the market has continued to evolve and the COSO Framework is evolving with it
- The update will address the call for:
  - Elevating enterprise risk management concepts and practices as the bar continues to rise
  - Incorporating lessons learned from recent crises
  - Responding to business and operating environments that are more complex, technologically driven, and global in scale
  - Increasing stakeholder engagement and greater transparency and accountability
  - Increasing prominence of discussions at the board level

The Project Update Goals

- Provide insight into strategy and the role of ERM when setting and executing strategy
- Enhance alignment between performance and ERM
- Accommodate expectation for governance and oversight
- Recognize globalization and need to apply a common albeit tailored approach
- Present new ways to view risk in setting and achieving objectives in the context of greater complexity
- Expand reporting to address greater transparency
- Accommodate evolving technology
Project Governance

- The Advisory Council is comprised of senior executives, academics and professional risk practitioners
- Observers include representatives from regulators and industry associations

ERM Update Approach and Timing

<table>
<thead>
<tr>
<th>Q3 2014</th>
<th>Q4 2014</th>
<th>Q2 2016</th>
<th>Q4 2016 - Q2 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess and Envision</td>
<td>Build and Design</td>
<td>Public Exposure</td>
<td>Finalization</td>
</tr>
</tbody>
</table>
What is Being Updated

- Revises the 2004 Enterprise Risk Management—Integrated Framework
- Includes both the core Framework and related Executive Summary
- The Application Techniques volume is not being updated
- Additional thought leadership will be considered by COSO in the future

Why Change the Title of the Framework

- Retitles the framework as Enterprise Risk Management—Aligning Risk with Strategy and Performance
- Recognizes the importance of strategy and entity performance
- Delineates between internal control and enterprise risk management
- Integrates enterprise risk management with decision making
Key Changes to the Framework

Top Changes to the Framework

- **Updates** components and **adopts** principles
- **Simplifies** definitions
- **Emphasizes** value
- **Renews** the focus on integration
- **Examines** role of culture
Top Changes to the Framework, continued

- **Elevates** discussion of strategy
- **Enhances** alignment with performance
- **Links** with decision making
- **Delineates** enterprise risk management from internal control
- **Refines** risk appetite and acceptable variation in performance

1. **Updates Components and Adopts Principles**
1. Updates Components and Adopts Principles

2. Simplifies Definitions

Risk

The possibility that events will occur and affect the achievement of strategy and business objectives

Enterprise Risk Management

The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value
3. Emphasizes Value

- Enhances the focus on value – how entities create, preserve, and realize value
- Embeds value throughout the framework, as evidenced by its:
  - Prominence in the core definition of enterprise risk management
  - Extensive discussion in principles
  - Linkage to risk appetite
  - Focus on the ability to manage risk to acceptable levels

4. Renews the Focus on Integration

- Integrates enterprise risk management with other business processes:
  - Governance Processes
  - Strategy Setting
  - Objectives Setting
  - Performance Management
- Focuses on applying enterprise risk management at various levels of the organization (e.g. entity level, business unit, division)
5. Examines the Role of Culture

- Addresses the growing focus, attention and importance of culture within enterprise risk management
- Influences all aspects of enterprise risk management
- Explores the relationship with culture in the context of:
  - Risk governance
  - Oversight of the entity
  - Connection between framework Components
- Depicts the behavior within a risk spectrum from risk averse to risk aggressive
- Affects the entity's decision making
- Explores the alignment of culture between individual and entity behavior

6. Elevates Discussion of Strategy

Explores enterprise risk management and strategy from three different perspectives:
- The **possibility** of strategy and business objectives not aligning with mission, vision and values
- The **implications from** the strategy chosen
- **Risk to** executing the strategy
7. Enhances Alignment with Performance

- Enables the achievement of business objectives by actively managing risk and performance
- Focuses on how risk is integral to performance by:
  - Exploring how enterprise risk management practices support the identification and assessment of risks that impact performance
  - Discussing acceptable variations in performance
- Manages risk in the context of achieving business objectives not as individual risks
- Seeks to enhance the integrated reporting on risk and performance

7. Enhances Alignment with Performance, continued

- Introduces a new depiction referred to as a risk profile
- Incorporates:
  - Risk
  - Performance
  - Risk appetite
  - Risk capacity
- Offers a dynamic and comprehensive view of risk and enables more risk-aware decision making
- The framework provides a complete depiction of how to build a risk profile
8. Links into Decision Making

- Explores how enterprise risk management drives risk aware decision making
- Highlights how risk awareness optimizes and aligns decisions impacting performance
- Explores how risk aware decisions affect the risk profile

9. Delineates Between Enterprise Risk Management and Internal Control

- The document does not replace the 2013 *Internal Control – Integrated Framework*
  - Most U.S. SEC registrants utilize the COSO *Internal Control Framework for Sarbanes Oxley compliance and as their framework for managing internal (financial) controls generally*
- The two frameworks are distinct and complementary
- Both use a components and principles structure
- Aspects of internal control common to enterprise risk management are not repeated
- Some aspects of internal control are developed further in this framework
10. Refines Risk Appetite and Acceptable Variation in Performance

- **Risk Appetite**: The amount of risk, on a broad level, an organization is willing to accept in pursuit of value

- **Acceptable Variation in Performance**: The boundaries of acceptable outcomes related to achieving business objectives

---

**Public Exposure Process**
Public Exposure Period

- Allowed for the development of awareness and acceptance by the public
- Provided the ability to gain input across:
  - Geography
  - Industry
  - Risk disciplines
- Extended from June 15, 2016 through September 30, 2016 and included:
  - Executive Summary
  - Framework
  - Appendices

Next Steps
Next Steps

1. Download draft framework at www.coso.org
   Framework expected to be finalized Q2 2017

2. Plan is to translate into: Chinese, Japanese, Spanish, French, Portuguese, Arabic and Russian

3. Stay connected with the Project Team at COSO-ERM_Update@us.pwc.com

4. Visit the www.coso.org website for further updates

Questions?